IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	**)**	
	)	
v.	**)**	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	**)**	
Defendant	**)**	

DEFENDANT'S REPLY TO GOVERNMENT'S RESPONSE TO MOTION TO SUPPRESS EVIDENCE OBTAINED FROM SEARCH OF INFORMATION ASSOCIATED WITH MR. CHATRIE'S GOOGLE ACCOUNTS

Okello Chatrie, through counsel, replies as follows to the government's response to his motions to suppress evidence obtained from the searches of information associated with his Google accounts. *See* ECF Nos. 20 and 42.

I. The Google account information warrant is fatally overbroad.

When the founders of our country wrote the Fourth Amendment, their concern was focused on prohibiting "general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists." *Stanford v. Texas*, 379 U.S. 476, 481 (1965). These general warrants had allowed customs officials to be able to search all manner of private places to ferret out goods that American colonists had imported without paying British taxes. *Id.* Early Americans so hated these general warrants because "they placed the liberty of every man in the hands of every petty officer" and were the "worst instrument[s] of arbitrary power." *Id.* The Fourth Amendment was intended to protect citizens from such general searches by requiring that a neutral judge find probable cause to seize and search for particular items.

The primary purpose of the particularity requirement was to eliminate the discretion of the police officers executing the search warrant as to what items the judge had authorized them to

seize. "As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Stanford*, 379 U.S. at 485-86 (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927).

When the government seizes, and the warrant purports to authorize seizure of, electronic data like the Google account information at issue here, the government has access to and possession of a trove of private information that would never be available in one location but for the advent of technology. The Supreme Court's decision in *Riley v. California*, 573 U.S. 373 (2015), recognizes that through electronic storage devices like cell phones, the "sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions." *Id.* at 394. "[T]here is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception." *Id.* at 395. "A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Id.* at 396-97.

There is nothing in the affidavit supporting the warrant that suggests that searching the entire Google account for essentially limitless "records and information," including all internet activity, is justified. The distinction that the government tries to draw between what it was authorized to search and what it was authorized to seize is meaningless. The volume of data that the government requested is not limited by anything other than a two and a half month period of time. Once the police reviewed the data, if anything appeared to them in plain view to be evidence of criminal activity, then, of course, they would seize that additional evidence too. That is the

problem with general warrants. General warrants authorize the government to pilfer through a vast volume of potential evidence to fish out pieces of evidence that may be useful in prosecuting a defendant. The Fourth Amendment explicitly prohibits such a fishing expedition. "Indeed, blanket suppression is warranted where the officers engage in a 'fishing expedition' for the discovery of incriminating evidence." *United States v. Uzenski*, 434 F.3d 690, 709 (4th Cir. 2006).

The affidavit lays out information about a bank robbery occurring and why the government believed that Mr. Chatrie was a suspect in that robbery. As Mr. Chatrie indicated in his motions, the affidavit in support of the warrant provides probable cause to search for mobile phone communications and location data immediately surrounding the robbery. *See* ECF No. 20 at 3-4. There is absolutely no specific, factual basis for the government to apply for or for the judge to authorize the expansive seizures and searches of Mr. Chatrie's entire Google account in this case. The only information even remotely connecting the robbery suspect to a Google account was an observation that the robber appeared to be on a cell phone around the time of the robbery, which provides probable cause to search for evidence of mobile phone communications and location data around the time of the robbery—nothing more.

The overbroad searches and seizures the warrant purported to authorize in this case leave only to the officer's discretion what items of evidence should be seized from the phones and slightly less broadly from electronic devices. As the Supreme Court recognized many decades ago, the Fourth Amendment requires a "neutral and detached" judge to find probable cause because the investigating officers are engaged in "the often competitive enterprise of ferreting out crime." *Coolidge*, 403 U.S. at 449 (quoting *Johnson v. United States*, 333 U.S. 10, 13-14 (1948)). "[T]he whole point of the basic rule so well expressed by Mr. Justice Jackson is that prosecutors and policemen simply cannot be asked to maintain the requisite neutrality with regard to their own

investigations—the 'competitive enterprise' that must rightly engage their single-minded attention." *Id.* at 450. Thus, it is the role of only the courts to enforce the constitutional requirement of particularity.

The government's expected reliance on the good faith argument does not save these warrants. *See, e.g., United States v. Marcus*, 807 F. Supp. 934, 935 (E.D.N.Y. 1992) (finding good faith inapplicable to warrant based on probable cause to search for four pornographic slides where warrant did not even describe slides and greatly expanded the types of information and items that could be searched and seized); *Cassady v. Goering*, 567 F.3d 628, 643-44 (10th Cir. 2009) (rejecting qualified immunity and finding that no reasonable officer could have believed that impermissibly broad warrant complied with Fourth Amendment). Thus, the Court should suppress all evidence seized pursuant to the search of Mr. Chatrie's Google account data.

II. The search warrant of the Google account also lacked a sufficient nexus between the place to be searched and the alleged crime.

In analyzing the nexus issue in the Google account warrant, it is critical to remember that there is far more than a semantic difference between probable cause to search a particular place and probable cause to arrest a particular person. The affidavit in support of the Google account warrant lays out in detail the evidence the police obtained identifying Mr. Chatrie as a suspect in this case. Aside from his having a Google account, however, there is nothing but generalized assertions by the affiant that evidence of the crime would be found in Mr. Chatrie's Google account. "It does not follow, however, that probable cause for arrest would justify the issuance of a search warrant, or, on the other hand, that probable cause for a search warrant would necessarily justify an arrest. Each requires probabilities as to somewhat different facts and circumstances—a point which is seldom made explicit in the appellate cases." *Zurcher v. Stanford Daily*, 436 U.S.

547, 556 n.6 (1978) (quoting LaFave, Search and Seizure: "The Course of True Law . . . Has Not . . . Run Smooth," U. Ill. Law Forum (1966)).

Simply because a criminal suspect has a digital media account does not give the government the right to search it for evidence of the suspected crime. Rather, there must be particularized information tying the place to be searched to the items to be seized. "The fact that there is probable cause to arrest a person for a crime does not automatically give police probable cause to search his residence or other area in which he has been observed for evidence of that crime." *United States v. Savoca*, 739 F.2d 220, 224 (6th Cir. 1984). Were the rule to be the opposite, there would be no distinction between probable cause to arrest and probable cause to search anything to which the suspect happens to have a connection. *Id.* at 225. As discussed above, however, probable cause to arrest and probable cause to search a place for evidence of a crime are distinct analyses—distinct, as applicable here, because the Fourth Amendment requires sufficient, particularized evidence that a nexus exists between the place to be searched and the items to be seized. Because here there was not a sufficient nexus to the expansive evidence sought in the Google account warrant, the Court must suppress evidence found therein.

CONCLUSION

The Court must find that the warrant was overbroad and that the affidavit did not provide a sufficient nexus to show that evidence of the alleged crime would be found on the expansive list of items to be searched. As such, the Court must suppress all evidence gained from the Google accounts.

Respectfully submitted,
OKELLO T. CHATRIE

By: /s/
Laura Koenig
Va. Bar No. 86840

Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on November 25, 2019, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

_____/s/_____
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org